AGENCY OF HUMAN SERVICES

AHS Disaster Recovery Standard

Jack Green

10/3/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Disaster Recovery (CP-1, CP-2(1), CP-4(1), CP-6, CP-6(1), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(5), CP-8, CP-8(1), CP-8(2), CP-9, CP-9(1), CP-10, CP-10(2), CP-10(3)) Controls.

Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
10/8/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Disaster Recovery (CP-1, CP-2(1), CP-4(1), CP-6, CP-6(1), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(5), CP-8, CP-8(1), CP-8(2), CP-9, CP-9(1), CP-10, CP-10(2), CP-10(3)) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

STANDARD

Disaster Recovery Plan development

1. IT Disaster Recovery Plans are to be developed and designed to reduce the impact of a major disruption on key business functions and processes.
2. The Disaster Recovery Plans must address the following:
    - Requirements for alternative processing
    - Requirements for recovery capability of all major IT services and systems
    - Usage guidelines
    - Roles and responsibilities
    - Contact information
    - Procedures
    - Communication processes
    - Testing approach
    - Response and recovery requirements for different time frames (e.g., within the first 24 hours, the next 48 hours, fourth through seventh days and extended disaster period)
3. During development, the priorities must be established in recovery situations and be developed such that they keep costs at an acceptable level while remaining in compliance with regulatory and contractual requirements.

4. Ensure that the plan is kept up-to-date with respect to any changes such as:
    - Personnel changes
    - New system deployment
    - Relevant document updates to ensure business requirements are reflected
5. When the plan is updated, all stakeholders must immediately be notified of the changes to the plan.
6. The Disaster Recovery plan must be tested on an annual basis.
    - During testing, the plan must be tested to ensure all IT systems can be effectively recovered and all shortcomings addressed.
7. Regular training sessions are conducted regarding the roles and responsibilities of concerned parties in the event of an incident or a disaster.
8. The Disaster Recovery Plan will contain instructions on how that training is enhanced or distributed in the event any new requirements are brought about for the following:
    - Role changes
    - Responsibility changes
    - Communication processes
9. The Disaster Recovery Plan will contain a managed distribution strategy.
    - All authorized parties must receive the plan and the distribution strategy
        i. The distribution strategy must account for all disaster scenarios.

IT Services Recovery and Resumption

1. When creating the Disaster Recovery Plan, there must be specific instructions for the recovery and resumption of the servers rendered by the Information System such as:
    - Activation of backup sites
    - Initiation of alternative processing
    - Customer and stakeholder communication
    - Resumption procedures

Post resumption review

1. After the successful resumption of the IT functions following a disaster, a post-resumption review must occur.
2. During this review, the adequacy of the Disaster Recovery Plan is assessed. If any inadequacies are found, the plan and procedures must be updated accordingly.

Alternate Storage Site Designation

1. An alternate storage site must be established for the storage and recovery of the information system’s backup information.

2. The alternate storage site must be in a location that is separate from the primary facility.
    - It must be separated from the primary facility to ensure that the risk of a disruption impacting both the primary and alternate site is low or otherwise is at an acceptable level, based on an assessment of risk.
    - Equivalent or related hazards or risks associated with the primary site must be absent or mitigated at the alternate storage site.
    - Potential problems with access to the alternate storage site in the event of an area-wide disruption or disaster must be identified and explicit mitigation actions must be outlined.
3. Agreements must be in place with the alternate storage site.
    - The agreements must detail service levels to be provided.
    - The agreements must include confidentiality and FTI requirements per federal guidelines.
4. The Contingency Plan for the information system must document the following regarding alternate storage sites:
    - The location of the alternate storage site, including the full address and contact information.
    - The agreements for use of the alternate storage site.
    - Hazards or risks associated with the alternate storage site and mitigations to address them.
    - Mitigation actions to address potential problems with access to the alternate storage site.
5. A log of all backup information stored at or retrieved from the alternate storage facility must be maintained.

Alternate Processing Site Designation

1. An alternate processing site for the information system established to permit the resumption of information system operations for essential missions and business functions.
2. A timeframe for resuming those essential functions when the primary processing capabilities are unavailable needs to be established.
    - The timeframe to resume information system operations remains consistent with return to operation standards for the information system established in the business impact analysis.
    - This timeframe is documented in the System Security Plan (SSP) for the information system, in the implementation description for this control.
3. Agreements must then be put in place with the alternate processing site once identified and vetted.

    - The alternate processing site will provide a Service Level Agreement (SLA) that contains priority-of-service provisions in accordance with the information system's requirements in the event of a disruption or disaster.
    - The alternate processing site agreement includes testing time that is sufficient to test the longest RTO of the critical MAs.
    - The agreement includes confidentiality requirements per federal guidelines.
4. Once established, the Contingency Plan for the information system then needs to be updated with the following requirements for alternate processing site:
    - The location of the alternate processing site, including the full address and contact information.
    - The agreements for use of the alternate processing site.
    - The criteria for activating the plan and achieving recovery at the alternate site.
    - Hardware, software, and telecommunications requirements for recovery at the alternate site.
    - Strategies for recovery at the alternate site.
    - Any relevant vendor contracts.
5. Finally, arrangements must be made to ensure the necessary equipment and supplies required to resume operations identified as priorities in the Contingency Plan are available in time to support the organization-defined time period for resumption.

Alternate Telecommunication Services Designation

1. Alternate telecommunications services are obtained with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.
2. The timeframe for resuming information system operations for essential missions and business functions using the alternate telecommunications services when the primary telecommunications capabilities are unavailable are available immediately.
3. The necessary telecommunications agreements must be developed with both primary and alternate service providers.
4. Once established, the Contingency Plan for the information system then needs to be updated with the following requirements for alternate telecommunication services:
    - The timeframe for the alternate telecommunications services to begin providing telecommunications capabilities when the primary telecommunications capabilities are unavailable.
    - Channels for necessary communications within EPA and between EPA and other organizations involved.
    - The names of the primary and the alternate telecommunications services providers and points of contact.
    - The agreements with the primary and alternate telecommunications service providers.

Information System Backup

1. Backups of user-level and system-level information contained in the information system are conducted.
2. Backups of information system documentation including security-related documentation are also conducted.
3. The frequency of information system backups must be consistent with the information systems' return to operation timeframes.
    - Incremental backups must be conducted daily.
    - Full backups must be conducted at least weekly.
4. The confidentiality and integrity of the system backup information must be protected at the storage location.
5. The information system's assessment of risk or information content must guide the use of encryption for protecting backup information.
6. Procedures for backing up and restoring the information system must be documented and included as attachments to the Contingency Plan.
7. Backup and restoration procedures must address the following:
    - Backups must be performed outside of regular business hours.
    - A routine schedule must be established for backing up user-level and system-level information.
    - All backup media must include markings that address the contents of the media, date created, and sequence number, if multiple media were used.
        i. For FTI, the backup tapes that contain FTI data are marked, logged, and transported security using two berries and a separate transmittal.
        ii. For FTI, the backup tapes are inventoried on a semi-annual basis.
    - The priorities and sequencing of restoration must be established.
    - Utilities must be used by personnel responsible for storage management in order to perform system backups and disk file restorations on production systems.
    - Each network access control device's configuration (e.g., system software, configuration data, and database files) must be backed up via a scheme that provides 100% recovery in case of system failure.
8. Backup information must be retained as follows:
    - Daily backups must be retained for at least two weeks.
    - Weekly backups must be retained for at least 90 days or in accordance with records retention requirements before being reused.

Offsite Backup Storage

1. The System Owner must ensure that all backup media, documentation and any other applicable IT resources necessary for recovery or resumption are off-site.

2. Process for backing up the data and the rotation schemes must be adequate to provide the required data for recovery with data loss minimization ensured.
3. IT Management ensures that off-site arrangements are assessed periodically (annually at minimum) for the following:
    - Content
    - Environmental protection
    - Security
4. The System Owner must ensure that the hardware used to restore from backup is tested as part of the Disaster Recovery Plan testing strategy.

IMPORTANT INFORMATION

These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec